



별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출원 번호 : 10-2003-0015526
Application Number

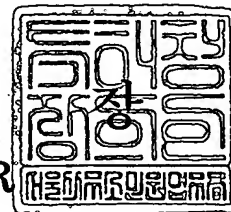
출원 년 월 일 : 2003년 03월 12일
Date of Application MAR 12, 2003

출원인 : 엘지전자 주식회사
Applicant(s) LG Electronics Inc.



2004 년 02 월 18 일

특 허 청
COMMISSIONER



【서지사항】

【서류명】	특허출원서		
【권리구분】	특허		
【수신처】	특허청장		
【참조번호】	0004		
【제출일자】	2003.03.12		
【발명의 명칭】	지티피 자원 추적 방법		
【발명의 영문명칭】	Method for Tracing GPRS Tunnel Protocol Resource		
【출원인】			
【명칭】	엘지전자 주식회사		
【출원인코드】	1-2002-012840-3		
【대리인】			
【성명】	김영철		
【대리인코드】	9-1998-000040-3		
【포괄위임등록번호】	2002-027003-6		
【대리인】			
【성명】	김순영		
【대리인코드】	9-1998-000131-1		
【포괄위임등록번호】	2002-027004-3		
【발명자】			
【성명의 국문표기】	김태용		
【성명의 영문표기】	KIM, TAE YONG		
【주민등록번호】	751024-1041514		
【우편번호】	442-710		
【주소】	경기도 수원시 팔달구 매탄동 주공1단지 APT.36동 307호		
【국적】	KR		
【심사청구】	청구		
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사를 청구합니다. 대리인 김영철 (인) 대리인 김순영 (인)		
【수수료】			
【기본출원료】	20	면	29,000 원
【가산출원료】	20	면	20,000 원

1020030015526

출력 일자: 2004/2/20

【우선권주장료】	0	건	0	원
【심사청구료】	12	항	493,000	원
【합계】	542,000			원
【첨부서류】	1.	요약서·명세서(도면)_1통		

【요약서】**【요약】**

본 발명은 SGSN(Serving GPRS Support Node)과 GGSN(GPRS Gateway Serving Node)간에 트래픽되는 GTP(GPRS Tunnel Protocol) 사용자 메시지의 점유 자원들을 추적하는 방법에 관한 것으로서, 추적 대상 가입자의 TEID를 이용하여 상기 가입자 메시지의 점유 자원에 대한 추적 기능을 설정하는 단계와; 상기 추적 기능이 설정된 가입자 메시지를 검출하여 해당 점유 자원에 대한 정보를 출력하는 단계를 포함하는 것을 특징으로 함으로써, 실제 가입자 데이터인 GTP-U 메시지에 할당된 GTP 자원을 파악하여 SGSN에서 발생하는 패킷 장애에 용이하게 대처할 수 있고, 인터넷 상에서의 GTP-U를 통한 DDOS 등의 공격에 대해서 해당 공격이 발생하는 인터페이스만을 격리시킴으로써 효과적으로 대처할 수 있으며, 추적 기능 지속 시간과 추적 임계값을 통해 자동으로 GTP-U 추적을 중지시킴으로써 시스템에 발생할 수 있는 처리 성능 저하를 방지할 수 있는 효과가 있다.

【대표도】

도 7

【명세서】

【발명의 명칭】

지티피 자원 추적 방법{Method for Tracing GPRS Tunnel Protocol Resource}

【도면의 간단한 설명】

도 1은 종래 GTP 자원 추적 시스템의 구성 블록도.

도 2는 종래 추적 정보 DB의 구조를 도시한 도.

도 3은 종래 GTP-C 추적 기능 설정 동작을 설명하기 위한 순서도.

도 4는 종래 GTP-C 추적 동작을 설명하기 위한 순서도.

도 5는 본 발명에 따른 GTP 자원 추적 시스템의 구성 블록도.

도 6은 본 발명에 따른 추적 정보 DB의 구조를 도시한 도.

도 7은 본 발명에 따른 GTP-U 추적 동작을 설명하기 위한 순서도.

도 8은 도 7에 있어, GTP-U 추적 기능 설정을 위한 호 추적부의 동작을 설명하기 위한 순서도.

도 9는 도 7에 있어, GTP-U 추적 기능 설정을 위한 호 처리부의 동작을 설명하기 위한 순서도.

도 10은 도 7에 있어, 패킷 처리부의 GTP-U 추적 동작을 설명하기 위한 순서도.

도 11은 도 7에 있어, 호 추적부의 GTP 자원 정보 출력 동작을 설명하기 위한 순서도.

도 12는 본 발명의 일실시예에 따른 GTP-U 추적을 위한 제어 흐름도.

* 도면의 주요 부분에 대한 부호의 설명 *

10 : SGSN

20 : GGSN(20)

- | | |
|---------------|-------------|
| 21 : SGSN 정합부 | 22 : 패킷 처리부 |
| 23 : 인터넷 정합부 | 24 : 호 추적부 |
| 25 : 추적 정보 DB | 26 : 호 처리부 |
| 30 : MMI | |

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<19> 본 발명은 GTP(GPRS Tunnel Protocol) 자원 추적 방법에 관한 것으로, SGSN(Serving GPRS Support Node)과 GGSN(GPRS Gateway Serving Node)간에 트래픽되는 GTP 사용자 메시지의 점유 자원들을 추적하여 외부에서 GGSN으로의 DDOS(Distributed Denial of Service) 등의 공격이나, 특정 가입자의 패킷 전달 불량등에 대해서 정확하게 대처할 수 있도록 하는 방법에 관한 것이다.

<20> 일반적으로 이동 단말기에 패킷 서비스를 제공하는 GPRS 서빙 노드인 SGSN과 IP 기반의 GPRS 백본망으로 연결되고, 외부 패킷 데이터 망(인터넷)에 직접 접속하여 터널링 및 라우팅 기능을 수행하는 GGSN은 첨부한 도면 도 1에 도시된 바와 같이 SGSN 정합부(21)와 패킷 처리부(22), 인터넷 정합부(23) 및 호 처리부(26)로 구성된다.

<21> 호 처리부(26)는 가입자의 호 설정 요구시 패킷 처리부(22) 및 SGSN(10)과 연동해 GTP 제어 메시지(GTP Control Message: GTP-C)를 이용하여 SGSN(10)과 SGSN 정합부(21) 사이에 터

널을 생성하고, 생성된 터널을 통해 가입자 데이터인 GTP 사용자 메시지(GTP User Message: GTP-U)를 트래픽시킨다.

- <22> 또한, GGSN(20)에는 MMI(Man Machine Interface)(30)를 통해 운용자로부터 특정 가입자에 대한 호 추적 요구가 수신되면 해당 GTP-C를 추적하여 해당 메시지가 점유한 자원 정보(이하 "GTP 자원 정보"라고 칭함)를 운용자에게 보고하는 호 추적부(24)와 현재 진행중인 호 추적에 대한 정보가 저장되는 추적 정보 DB(25)가 포함된다.
- <23> 호 추적부(24)는 운용자의 호 추적 요구 수신시 해당 메시지에 포함된 추적 대상 가입자의 식별 정보(이하 "추적 정보"라고 칭함)를 추적 정보 DB(25)에 저장하여 GTP-C 추적 기능을 설정하고, 호 처리부(26)로부터 GTP 자원 정보 수신시 이를 MMI(30)를 통해 운용자에게 보고한다.
- <24> 호 처리부(26)는 GTP-C 수신시 상기 추적 정보 DB(25)에서 해당 가입자에 대한 GTP-C 추적 기능 설정 여부를 검색하여 해당 기능이 설정되어 있는 경우 해당 GTP 자원 정보를 호 추적부(24)로 송신한다.
- <25> 상기 호 추적부(24)에 의해 추적 정보가 저장되고 GTP-C 추적시 호 처리부(26)에 검색되는 추적 정보 DB(25)에는 도 2에 도시된 바와 같이, 저장되는 추적 정보의 인덱스 필드(INDEX)와, 추적 대상 가입자 번호인 IMSI(International Mobile Subscriber Identifier) 필드(IMSI), 해당 가입자 번호의 자릿수를 나타내는 IMSI 자릿수 필드(IMSI_CNT), 해당 가입자의 IP(Internet Protocol) 주소가 저장되는 IP 주소 필드(IP_ADDR) 및 해당 추적 타입을 의미하는 추적 타입 필드(TRC_TYPE)가 구비된다.
- <26> 상기 추적 타입 필드(TRC_TYPE)의 상세한 구조는 아래의 표와 같다.

<27> 【표 1】

비트8	비트7	비트6	비트5	비트4	비트3	비트2	비트1
Priority	Reserved	BSS Record Type		SGSN Record Type		Invoking Event	

- <28> 상기 표 1을 참조하면, GTP-C 추적과 관련하여 호 추적 발생 이벤트인 인보킹 이벤트 (Invoking Event) 비트 각각에는 GSM12.08에 명시된 바와 같이 개발자가 상기 비트3 내지 비트 7을 임의로 사용할 수 있음을 의미하는 1이 세팅된다.
- <29> 그리고, SGSN 레코드 타입(SGSN Record Type) 비트는 각각 해당 추적 타입이 호 감시인 경우 0, 1로 세팅되고 호 추적인 경우 모두 0으로 세팅되며 추적 기능 해제인 경우 1, 1로 세팅된다. 상기 호 감시는 추적 대상 가입자의 호가 종료된 다음에 해당 호에 대한 통화시간 및 가입자의 위치 정보 등을 출력하는 타입이고, 호 추적은 GTP-C가 수신될 때마다 해당 메시지를 출력하는 타입을 의미한다.
- <30> 이하, GGSN(20)에서 GTP-C 추적 동작을 첨부한 도면을 참조하여 설명한다.
- <31> 도 3은 호 추적부(24)의 GTP-C 추적 기능 설정 동작을 설명하기 위한 순서도로서 도 3을 참조하면, 호 추적부(24)는 운용자의 GTP-C 추적 요구 메시지를 MMI(30)를 통해 수신한다. (S301). 상기 GTP-C 추적 요구 메시지에는 추적 대상 가입자의 IMSI 또는 IP 주소와 추적 타입 등에 대한 추적 정보가 저장된다.
- <32> 해당 GTP-C 추적 요구 메시지를 수신한 호 추적부(24)는 수신된 메시지를 분석하여 해당 메시지에 실린 추적 정보를 추적 정보 DB(25)에 저장한다(S302). 그 후, 추적 정보 DB(25)에 상기 추적 정보가 성공적으로 저장되어 설정이 완료되면 운용자에게 GTP-C 추적 기능 설정 성

공 메시지를 출력하며(S303,S304), 상기 정보 저장에 실패했을 경우 GTP-C 추적 기능 설정 실패 메시지를 출력한다(S303,S305).

<33> 도 4는 상기와 같이 GTP-C 추적 기능이 설정된 가입자에 대한 GTP-C 추적 동작을 설명하기 위한 순서도이다.

<34> 도 4를 참조하면, 패킷 처리부(22)를 통해 SGSN(10)측으로부터 GTP-C를 수신하는 호 처리부(26)는 패킷 처리부(22)와 인터넷 정합부(23)의 자원 가용성 여부 판단 및 기타 호 처리 절차를 수행하고 해당 결과를 가입자 측으로 송신한다(S401).

<35> 이때, 호 처리부(26)는 추적 정보 DB(25)를 검색하여 해당 가입자에 대한 GTP-C 추적 기능 설정 여부를 확인한다(S402).

<36> 상기 확인 결과, 해당 기능이 설정되어 있는 경우(S403), 추적 정보 DB(25)의 추적 타입을 확인하여 해당 추적 타입이 호 추적인 경우 수신된 GTP-C를 호 추적부(24)로 송신하고(S404,S405), 해당 추적 타입이 호 감시인 경우 해당 호가 해제된 다음에 통화 종료 시간과 가입자 위치정보 등을 호 추적부(24)로 송신한다(S404,S406).

<37> 이에, 호 추적부(24)는 상기 GTP-C 수신시 현재 진행되고 있는 호의 상태를 운용자에게 보고하고(S407), 해당 호 해제시 수신되는 통화 종료 시간과 가입자 위치 정보 등을 운용자에게 보고한다(S408).

<38> 전술한 바와 같이 기존의 호 추적은 GTP-C에 대해서만 이루어지기 때문에 실제 사용자 데이터인 GTP-U에 대해서는 교환기 내부의 점유 자원에 대해서 추적이 되지 않는다.

<39> 이는 SGSN에서 전달되어지는 패킷에 장애가 발생할 경우 정확하게 어떤 정합부에서 장애가 발생했는지를 감지할 수 없기 때문에 교환기 운용자의 장애 대처(trouble shooting)에 어려움을 발생시킨다.

<40> 더욱이, 인터넷으로부터 트래픽되는 GTP-U의 경우 해당 메시지가 DDOS 등의 공격일 경우 공격받고 있는 인터페이스를 식별할 수 없기 때문에 빠른 대처가 불가능하여 교환기 전체의 안정성 및 신뢰성에 심각한 장애를 발생시킬 수 있는 문제점이 있었다.

【발명이 이루고자 하는 기술적 과제】

<41> 본 발명은 전술한 바와 같은 문제점을 해결하기 위한 것으로 그 목적은, 추적 대상 가입자의 TEID를 이용해 실제 가입자 데이터인 GTP-U를 추적함으로써, 해당 GTP-U에 할당된 GTP 자원을 파악하는데 있다.

【발명의 구성 및 작용】

<42> 상술한 바와 같은 목적을 달성하기 위한 본 발명의 GTP 자원 추적 방법은, 추적 대상 가입자의 TEID를 이용하여 상기 가입자 메시지의 점유 자원에 대한 추적 기능을 설정하는 단계와; 상기 추적 기능이 설정된 가입자 메시지를 검출하여 해당 점유 자원에 대한 정보를 출력하는 단계를 포함하는 것을 특징으로 한다.

<43> 바람직하게는, 상기 추적 기능을 설정하는 단계는 호 추적부에서 운용자로부터 수신되는 상기 가입자에 대한 추적 정보를 호 처리부로 송신하는 단계와; 상기 호 처리부에서 상기 추적 정보를 이용해 상기 가입자에게 할당된 TEID를 검색하는 단계와; 상기 TEID를 이용해 패킷

처리부에 상기 가입자 메시지 추적 기능을 등록하고 상기 TEID를 호 추적부로 송신하는 단계와; 상기 호 추적부에서 상기 TEID를 상기 추적 정보와 함께 추적 정보 DB에 저장하는 단계를 포함하는 것을 특징으로 한다.

<44> 바람직하게는, 상기 추적 정보는 상기 가입자의 IMSI, IP 주소, 가입자 메시지 추적을 지시하는 추적 타입 및 추적 대상 메시지의 최대값인 추적 임계값 정보를 포함하는 것을 특징으로 하며, 상기 추적 정보 DB에는 추적 정보, TEID 및 추적된 메시지 개수인 추적 카운트값이 저장되는 것을 특징으로 한다.

<45> 바람직하게는, 상기 TEID 등록은 상기 패킷 처리부에서 상기 TEID와 추적 정보를 수신하는 단계와; 내부 TEID 테이블에서 해당 TEID 필드의 추적 플래그를 활성화시키고 상기 추적 정보를 저장하는 단계를 포함하는 것을 특징으로 한다.

<46> 또한 바람직하게는, 상기 점유 자원 정보를 출력하는 단계는 패킷 처리부에서 트래픽되는 가입자 메시지의 TEID를 확인하는 단계와; 상기 확인된 TEID로 내부 TEID별 테이블을 검색하여 상기 TEID의 추적 플래그 활성 여부를 확인하는 단계와; 상기 추적 플래그가 활성 상태인 경우 상기 가입자 메시지의 점유 자원에 대한 정보를 상기 TEID와 함께 호 추적부로 송신하는 단계와; 상기 호 추적부에서 상기 TEID를 이용해 상기 점유 자원 정보를 운용자에게 출력하는 단계를 포함하는 것을 특징으로 한다.

<47> 바람직하게는, 상기 점유 자원 정보는 상기 가입자 메시지가 트래픽되는 AMA 번호, 인터페이스 번호, VPI/VCI, 링크 대역, 상기 데이터의 스트림 방향성 지시값 및 추적 카운트값을 포함하는 것을 특징으로 한다.

- <48> 바람직하게는, 상기 점유 자원 정보를 운용자에게 출력하는 단계는 상기 호 추적부에서 추적 정보 DB를 검색하여 상기 TEID가 저장되어 있는지 여부를 확인하는 단계와; 상기 TEID가 저장되어 있는 경우 상기 점유 자원 정보를 상기 TEID에 대응하는 가입자 추적 정보에 매핑시켜 운용자에게 출력하는 단계와; 상기 호 추적 정보 DB에서 추적 카운트값을 증가시키고, 기저장된 추적 임계값과 비교하는 단계와; 상기 추적 카운트값이 상기 추적 임계값과 동일한 경우 상기 추적 정보 DB에서 상기 TEID 및 대응하는 추적 정보를 삭제하는 단계를 포함하는 것을 특징으로 한다.
- <49> 또한 바람직하게는, 상기 운용자로부터 수신되는 추적 정보에 해당 추적 기능을 지속할 시간 정보가 포함되어 있는 경우, 상기 호 추적부에서 상기 TEID 수신시 상기 지속 시간에 대응하는 타이머를 구동시키는 단계를 더 포함하는 것을 특징으로 한다.
- <50> 바람직하게는, 상기 타이머가 만료하는 경우 상기 호 추적부에서 상기 추적 정보 DB의 상기 TEID 및 대응하는 추적 정보를 삭제하여 해당 가입자 메시지 추적 기능을 해제하는 것을 특징으로 한다.
- <51> 또한 바람직하게는, 상기 가입자의 호가 해제되는 경우 상기 설정된 추적 기능을 해제하는 단계를 더 포함하는 것을 특징으로 하며, 상기 추적 기능을 해제하는 단계는 호 처리부에서 상기 호 해제된 가입자의 식별 정보가 포함된 세션 종료 통지를 호 추적부로 송신하는 단계와; 상기 호 추적부에서 상기 식별 정보를 이용해 추적 정보 DB의 해당 TEID 및 추적 정보를 삭제하여 상기 가입자 메시지 추적 기능을 해제하는 단계를 포함하는 것을 특징으로 한다.

- <52> 이하, 본 발명에 따른 바람직한 실시예를 첨부한 도면을 참조하여 상세하게 설명한다.
다만, GTP-C 추적 방법은 종래와 동일하므로 그 설명을 생략한다.
- <53> 본 발명의 일실시예에 따른 GTP-U 추적 시스템은 도 5에 도시된 바와 같이 그 전체적인 구성에 있어서 종래와 동일하다. 다만, 호 추적부(24)는 MMI(30)를 통해 운용자로부터 특정 가입자의 GTP-U 점유 자원에 대한 추적 요구인 GTP-U 추적 요구를 수신한다.
- <54> 상기 GTP-U 추적 요구에는 추적 정보가 포함되는데, 상기 추적 정보는 IMSI 또는 IP 주소, 추적 타입, 추적 임계값 등이고, 나아가 추적 기능 지속 시간 정보가 포함될 수 있다.
- <55> IMSI는 가입자 식별 번호를 의미하며, IP는 해당 가입자가 인터넷을 통한 호를 하기 위해서 할당되어지는 주소를 의미한다. 그리고 추적 타입은 해당 추적이 수행되는 방식으로, GTP-U 추적의 경우 전술한 표 1의 인보킹 이벤트 비트와 SGSN(10) 레코드 타입 비트가 아래의 표와 같이 세팅될 수 있다.

<56> 【표 2】

추적타입	Bit4	Bit3	Bit2	Bit1
GTP-U 추적	0	1	1	1

- <57> 추적 임계값은 GTP-U 추적시 추적되는 메시지의 개수 제한을 위한 파라미터(Parameter)로서 메시지가 트래픽되는 방향에 따라 업 스트림 임계값과 다운 스트림 임계값이 있다. 업 스트림 임계값은 SGSN(10)에서 인터넷 방향으로 트래픽되는 추적 대상 메시지 개수의 최대값을 의미하고, 다운 스트림 임계값은 인터넷에서 SGSN(10) 방향으로 트래픽되는 추적 대상 메시지 개수의 최대값을 의미하는 것으로, 추적되는 메시지의 개수(카운트 값)가 추적 임계값 이상이 되면 해당 방향에 대한 GTP-U 추적은 종료한다.

- <58> 추적 기능 지속 시간은 시스템의 성능을 위해서 과도한 추적이 진행되는 것을 방지하기 위한 파라미터로서 GTP-U 추적이 지속되는 시간을 의미한다. 따라서, 추적 기능 지속 시간을 초과하게 되면, 상기 추적 임계값 이하인 경우에도 GTP-U 추적은 종료한다.
- <59> 그리고, 호 추적부(24)는 상기 수신된 추적 정보 중 IMSI 또는 IP 주소, 추적 임계값을 호 처리부(26)로 송신하여 GTP-U 추적 기능 등록을 요구하고, 상기 추적 기능이 등록된 경우 상기 추적 정보와, 추적 기능 등록과 함께 호 처리부(26)로부터 수신되는 TEID(Tunnel Endpoint Identifier)를 추적 정보 DB(25)에 저장하여 GTP-U 추적 기능을 설정하며, 패킷 처리부(22)로부터 GTP-U 추적 결과인 GTP 자원 정보가 수신되는 경우 이를 추적 대상 가입자의 IMSI, IP 주소에 매핑시켜 MMI(30)를 통해 운용자에게 보고한다.
- <60> 상기 TEID는 SGSN(10)과 SGSN 정합부(21)의 GTP-U 레이어(Layer) 간에 생성되어 각각의 호 마다 할당되어지는 다수의 가상 터널을 구분하는 터널 종단점 식별자이다.
- <61> 도 6은 상기 추적 정보 DB(25)의 구조를 예시한 도면으로서, 추적 정보 DB(25)에는 추적 정보 인덱스(INDEX), 추적 대상 가입자의 IMSI, IMSI의 자릿수(IMSI_CNT), IP 주소(IP_ADDR), 추적 타입(TRC_TYPE), 호 처리부(26)로부터 수신되는 상기 IMSI 또는 IP 주소에 매핑된 TEID, 추적 카운트 값(Up/Down Stream CNT), 및 추적 임계값(Up/Down Stream LMT)이 저장되고, 운용자로부터 추적 기능 지속시간이 수신되는 경우 수신된 추적기능 지속 시간(DURATION)과 해당 지속 시간동안 구동하는 타이머 식별자(TIMER_ID)가 저장된다.
- <62> 다르게는, 상기 추적 정보 DB(25)는 종래 GTP-C 추적을 위한 추적 정보 DB와 별개의 DB로 구성될 수도 있다.

<63> 호 처리부(26)는 GTP-C 수신시 SGSN(10)과 연동하여 터널을 생성함으로써 가입자의 호를 설정하고, 아래의 표와 같은 가입자 정보 테이블을 이용해 IMSI 또는 IP 주소를 임의의 TEID에 매핑시켜 상기 생성된 터널을 통해 호 처리를 수행한다.

<64> 【표 3】

IMSI	IP 주소	TEID	가입자 프로파일
------	-------	------	----------

<65> 또한, 호 처리부(26)는 호 추적부(24)로부터 IMSI 또는 IP 주소, 추적 임계값 등의 추적 정보가 포함된 GTP-U 추적 기능 등록 요구가 수신되면, 상기 가입자 정보 테이블에서 상기 IMSI 또는 IP 주소에 매핑된 TEID를 검색하여 상기 추적 정보와 함께 패킷 처리부(22)로 송신함으로써 GTP-U 추적 기능을 등록시키고, 상기 검색된 TEID를 호 추적부(24)로 송신한다.

<66> 패킷 처리부(22)는 아래의 표와 같은 TEID 테이블을 이용하여 SGSN 정합부(21)를 통해 수신되는 GTP-U를 라우팅하여 인터넷 정합부(23)를 통해 인터넷(도면에 도시되지 않음)으로 송신하며, 인터넷 정합부(23)를 통해 수신되는 GTP-U를 라우팅하여 SGSN 정합부(21)를 통해 SGSN(10)으로 송신한다.

<67> 【표 4】

TEID	IP주소	QoS	스트림대역(Up/Down)	추적플래그	추적임계값	추적카운트값
------	------	-----	----------------	-------	-------	--------

<68> 또한, 패킷 처리부(22)는 GTP-U 추적 기능 등록과 관련하여 호 처리부(26)로부터 TEID와 추적 정보가 수신되는 경우 상기 TEID 테이블의 해당 필드에 상기 추적 정보(추적 임계값)를 저장하고, 추적 플래그를 활성화시킨다.

<69> 그리고, 상기 TEID를 가지는 GTP-U 검출시 해당 GTP 자원 정보를 추적 카운트값을 증가시키면서 추적 임계치만큼 호 추적부(24)로 송신하되, 추적 카운트값이 추적 임계치와 동일하게 되면 추적 플래그를 비활성화시키고 추적 카운트 값 및 추적 임계값을 삭제하여 해당 GTP-U 추적 기능을 해제한다.

<70> 상기 GTP 자원 정보에는 아래의 표와 같은 정보가 포함된다.

<71> 【표 5】

필드	내용
CNT	UP/DOWN 스트림에 대해 호 추적부에 보고한 회수
STREAM_DIR	스트림 방향
AMA_No	SGSN 정합부/인터넷 정합부의 AMA(ATM Management Assemble) 번호
INF_No	SGSN 정합부/인터넷 정합부의 인터페이스 번호
PORT_No	SGSN 정합부/인터넷 정합부의 포트 번호
VPI/VCI	SGSN 정합부/인터넷 정합부의 VPI/VCI 번호
LINK_BW	SGSN 정합부/인터넷 정합부의 UP/DOWN 스트림 링크 대역

<72> 도 7은 상기와 구성된 시스템의 GTP-U 추적 동작을 설명하기 위한 순서도이다.

<73> 도 7을 참조하면, 호 추적부(24)는 MMI(30)를 통해 운용자로부터 추적 대상 가입자에 대한 추적 정보가 포함된 GTP-U 추적 요구를 수신하고(S610), 해당 가입자에 대한 GTP-U 추적 기능을 설정한다(S620).

<74> 즉, 호 추적부(24)는 상기 추적 정보 중 IMSI 또는 IP 주소, 추적 임계치를 호 처리부(26)로 송신하여 GTP-U 추적 기능 등록을 요구하고, 호 처리부(26)는 상기 표 3과 같은 가입자 정보 테이블에서 호 추적부(24)로부터 수신된 IMSI 또는 IP 주소에 매핑된 TEID를 검색하여 검색된 TEID와 상기 추적 임계치를 패킷 처리부(22)로 송신하여 해당 TEID에 GTP-U 추적 기능을 등록하며, 상기 검색된 TEID를 호 추적부(24)로 송신한다.

- <75> 그러면, 호 추적부(24)는 운용자로부터 수신된 추적 정보와 호 처리부(26)로부터 수신된 TEID를 추적 정보 DB(25)에 저장함으로써 GTP-U 추적 기능을 설정하게 된다.
- <76> 한편, 패킷 처리부(22)는 SGSN 정합부(21) 및 인터넷 정합부(23)를 통해 트래픽되는 GTP-U를 추적하여 추적 대상 GTP-U 검출시 해당 메시지가 점유한 GTP 자원 정보를 호 추적부(24)로 송신하고(S640), 호 추적부(24)는 수신된 GTP 자원 정보를 MMI(30)를 통해 운용자에게 보고한다(S660).
- <77> 도 8은 상기 GTP-U 추적 기능 설정을 위한 호 추적부(24)의 동작을 설명하기 위한 순서도로서 도 8을 참조하면, 먼저 호 추적부(24)는 MMI(30)를 통하여 운용자가 입력한 GTP-U 추적 요구 메시지를 수신한다(S610). 해당 메시지에는 추적 대상 가입자에 대한 추적 정보인 IMSI 또는 IP 주소, 추적 임계값이 저장되고, 나아가 해당 추적 시간을 제한하기 위한 추적 기능 지속 시간 정보가 포함된다.
- <78> 그리고, 상기 수신된 추적 정보를 GTP-U 추적 기능 등록 요구 메시지에 저장한 다음 호 처리부(26)로 송신하여 GTP-U 추적 기능 등록을 요구한다(S621). 이때, 호 처리부(26)로부터 일정시간 동안 응답을 받지 못하는 경우 이를 감지하기 위해 TMR1 만큼의 타임아웃을 설정한다.
- <79> 그 후, 호 처리부(26)로부터 상기 GTP-U 추적 기능 등록 요구에 대한 응답 메시지를 수신하게 되면(S622), 응답 메시지에 저장된 결과값을 조사하여 결과값이 GTP-U 추적 기능 등록이 성공하여 패킷 처리부(22)에 현재 GTP-U 추적 플래그가 활성화되었음을 의미하는 값

(SUCCESS)이면, 운용자가 입력한 추적 정보에 포함된 추적 기능 지속 시간에 대응하는 타이머를 구동한다(S623, S624).

<80> 즉, 상기 추적 기능 지속 시간 만료를 통지하는 타이머 만료 시그널이 수신될 수 있도록 상기 GTP-U 추적 기능 등록 성공시 호 처리부(26)로부터 수신되는 TEID를 추적 기능 지속 시간과 함께 저장한 타이머 만료 시그널을 OS에 등록한다. 이때, 타이머 만료 시그널 등록에 실패한 경우 호 추적부(24)는 운용자에게 GTP-U 추적 기능 설정이 실패하였음을 보고한다.

<81> 그리고, 운용자로부터 수신된 추적 정보와 호 처리부(26)로부터 수신된 GTP-U 추적 기능 등록 요구 응답 메시지에 포함된 TEID를 추적 정보 DB(25)에 저장함으로써 운용자의 GTP-U 추적 요구에 따른 GTP-U 추적 기능 설정을 완료하게 된다(S625).

<82> 한편, 호 처리부(26)로부터 GTP-U 추적 기능 등록 요구에 대한 응답이 없거나(S622), 해당 GTP-U 추적 기능 등록 요구 응답 메시지의 결과값이 등록 실패를 의미하는 값(FAIL)인 경우(S623), 운용자에게 GTP-U 추적 기능 설정에 실패하였음을 보고한다(S626).

<83> 도 9는 GTP-U 추적 기능 설정을 위한 호 처리부(26)의 동작을 설명하기 위한 순서도로서 도 9를 참조하면, 호 처리부(26)는 호 추적부(24)로부터 GTP-U 추적 기능 등록 요구 메시지를 수신하고(S631), 해당 메시지에 포함된 추적 정보에서 IMSI 또는 IP 주소를 판독하여 해당 가입자의 호가 현재 존재하는지 여부를 확인한다(S632, S633).

<84> 상기 확인 결과, 해당 호가 존재할 경우 상기 표 3과 같은 가입자 정보 테이블을 검색하여 상기 IMSI 또는 IP 주소에 매핑된 TEID를 검색하고(S634), 검색된 TEID를 상기 추적 정보(추적 임계값)와 함께 패킷 처리부(22)로 송신하여 GTP-U 추적 기능을 등록한 다음(S635),

GTP-U 추적 기능 등록 요구 응답 메시지에 등록 성공을 알리는 결과값(SUCCESS)을 설정하여 상기 검색된 TEID와 함께 호 추적부(24)로 송신한다(S636).

<85> 한편, 상기 가입자 호 존재 여부 확인 결과(S633), 해당 호가 존재하지 않을 경우 GTP-U 추적 기능 등록 응답 메시지에 등록 실패를 알리는 결과값(FAIL)을 설정하여 호 추적부(24)로 송신한다(S637).

<86> 도 10은 패킷 처리부(22)의 GTP-U 추적 동작을 설명하기 위한 순서도로서 도 10을 참조하면, 먼저 패킷 처리부(22)는 호 처리부(26)로부터 GTP-U 추적 기능 등록과 관련된 TEID 및 추적 정보(추적 임계값)가 수신되면(S641), 상기 표 4와 같은 TEID 테이블에서 상기 수신된 TEID에 해당하는 추적 임계값 필드에 상기 수신된 추적 정보를 저장하고, 해당 추적 플래그를 활성화시킨다(S642).

<87> 그후, 패킷 처리부(22)는 SGSN(10) 정합부(21) 또는 인터넷 정합부(23)를 통해 트래픽되는 GTP-U를 수신하여 해당 메시지의 TEID를 확인하고, 확인된 TEID를 검색키로 TEID 테이블을 검색하여 해당 TEID에 대해 추적 플래그가 활성화 여부를 확인한다(S643, S644).

<88> 상기 확인 결과, 추적 플래그가 활성 상태인 경우, 상기 표 5와 같은 GTP 자원 정보를 해당 TEID와 함께 GTP 자원 정보 메시지에 저장하여 호 추적부(24)로 송신한다(S645, S646).

<89> 그리고, 상기 TEID 테이블의 해당 추적 카운트값을 1 증가시킨 다음(S647), 해당 추적 임계치와 비교하여(S648), 동일하지 않은 경우 다음 GTP-U 검출 동작을 수행하고(S644), 동일한 경우 TEID 테이블에서 추적 카운트값 및 추적 임계값을 삭제하고, 추적 플래그를 비활성화 시킴으로써 해당 GTP-U 추적 동작을 종료한다(S649).

- <90> 이때, 추적 카운트값과 추적 임계치의 비교는 업 스트림과 다운 스트림 각각 별개로 이루어진다. 따라서, 업 스트림과 다운 스트림 중 어느 하나의 추적 카운트 값이 추적 임계치와 동일한 경우 해당되는 스트림의 GTP-U 추적 동작만 종료하게 된다.
- <91> 도 11은 호 추적부(24)의 GTP 자원 정보 출력 동작을 설명하기 위한 순서도이다. 도 11을 참조하면, 추적 기능 지속 시간에 대응하는 타이머가 만료하지 않은 동안(S661), 호 추적부(24)는 패킷 처리부(22)로부터 수신되는 GTP 자원 정보 메시지에 포함된 TEID를 검색키로 하여 추적 정보 DB(25)에 해당 TEID가 저장되어 있는지 여부를 검색한다(S662, S663).
- <92> 상기 검색 결과, 상기 TEID가 추적 정보 DB(25)에 저장되어 있지 않은 경우 수신된 GTP 자원 정보 메시지를 폐기하고, 상기 TEID가 추적 정보 DB(25)에 저장되어 있는 경우 TEID에 매핑된 IMSI 또는 IP 주소를 상기 GTP 자원 정보 메시지에 포함된 GTP 자원 정보와 함께 MMI(30)를 통해 운용자에게 출력한다(S664).
- <93> 이때, 상기 GTP 자원 정보에는 패킷 처리부(22)의 TEID 테이블에 저장된 추적 카운트값이 포함되는데, 이 값은 추적 정보 DB(25)에 저장된 추적 카운트값과 동일한 값이다. 그러나, 패킷 처리부(22)와 호 추적부(24)의 동기 불일치 등으로 인하여 상기 값들이 불일치하는 경우 상기 GTP 자원 정보에는 추적 정보 DB(25)에 저장된 추적 카운트값이 포함된다.
- <94> 그리고, 상기 GTP 자원 정보를 출력한 호 추적부(24)는 추적 정보 DB(25)의 추적 카운트 값을 1 증가시킨 다음 추적 임계치와 비교하여(S665, S666), 추적 카운트값이 추적 임계치와 동일한 경우 추적 정보 DB(25)에 저장되어 있는 타이머 ID를 이용하여 타이머를 취소하고(S667),

추적 정보 DB(25)에서 해당 TEID 관련 데이터, 즉 추적 정보 및 추적 카운트값 등을 모두 삭제하여 해당 GTP-U 추적 동작을 종료한다(S668).

<95> 이때, 추적 카운트값과 추적 임계치의 비교는 업 스트림과 다운 스트림 각각 별개로 이루어진다. 따라서, 업 스트림과 다운 스트림 중 어느 하나의 추적 카운트값이 추적 임계치와 동일한 경우 해당되는 스트림의 GTP-U 추적 동작만 종료하게 된다.

<96> 한편, 호 추적부(24)는 추적 기능 지속 시간에 대응하는 타이머가 만료한 경우, 즉 OS에 등록된 타이머 만료 시그널이 수신되는 경우(S661), 상기 타이머 만료 시그널에 포함된 TEID를 검색키로 하여 추적 정보 DB(25)를 검색하여 해당 TEID 관련 데이터를 모두 삭제하여 해당 GTP-U 추적 동작을 종료한다(S668). 이때, 상기 TEID가 추적 정보 DB(25)에 존재하지 않으면 상기 타이머 만료 시그널을 폐기시킨다.

<97> 다른 한편, 호 추적부(24)는 추적 대상 가입자의 호가 해제되는 경우 호 처리부(26)로부터 세션(Session) 종료 통지 메시지를 수신하고, 해당 메시지에 포함된 IMSI 또는 IP 주소, TEID를 검색키로 하여 추적 정보 DB(25)를 검색하여 해당 TEID에 대응하는 추적 정보 및 추적 카운트 값 등 관련 데이터를 모두 삭제하여 해당 GTP-U 추적 동작을 종료한다.

<98> 또한, 운용자로부터 GTP-U 추적 기능이 설정된 특정 가입자에 대한 추적 기능 해제 요구가 있는 경우 전술한 GTP-U 추적 기능 설정과 동일한 과정을 거쳐 GTP-U 추적 기능을 해제한다.

<99> 도 12는 본 발명의 일실시예에 따른 GTP-U 추적을 위한 제어 흐름도이다.

- <100> 도 12를 참조하면, 호 추적부(24)는 MMI(30)를 통해 운용자로부터 추적 대상 가입자에 대한 추적 정보가 포함된 GTP-U 추적 요구 메시지를 수신하고(S1), 상기 추적 정보가 포함된 GTP-U 추적 기능 등록 요구 메시지를 호 처리부(26)로 송신한다(S2).
- <101> 호 처리부(26)는 상기 추적 정보에 포함된 IMSI 또는 IP 주소에 매핑된 TEID를 검색하여 상기 추적 정보와 함께 GTP-U 추적 기능 등록 요구 메시지에 저장하여 패킷 처리부(22)로 송신한다(S3).
- <102> 그러면, 패킷 처리부(22)는 상기 추적 정보를 내부 TEID 테이블에 저장하고 수신된 TEID에 대한 추적 플래그를 활성화시켜 GTP-U 추적 기능을 등록하고(S4), GTP-U 추적 기능 등록 응답 메시지를 호 처리부(26)로 송신한다(S5).
- <103> 상기 응답 메시지를 수신한 호 처리부(26)는 상기 검색된 TEID가 포함된 GTP-U 추적 기능 등록 응답 메시지를 호 추적부(24)로 송신하고(S6), 호 추적부(24)는 상기 응답 메시지에 포함된 TEID와 운용자로부터 입력된 추적 정보를 추적 정보 DB(25)에 저장함으로써 해당 가입자에 대해 GTP-U 추적 기능을 설정한다(S7).
- <104> 그 후, 패킷 처리부(22)는 등록된 TEID를 가지는 GTP-U 검출시(S8), 해당 메시지가 점유한 자원 정보 및 해당 TEID가 포함된 GTP 자원 정보 메시지를 호 추적부(24)로 송신하고(S9), 호 추적부(24)는 추적 정보 DB(25)에서 수신된 TEID에 매핑된 IMSI 또는 IP 주소를 검색하여 상기 GTP 자원 정보와 함께 GTP-U 추적 결과 메시지에 저장하여 MMI(30)를 통해 운용자에게 보고한다(S10).
- <105> 한편, 추적 대상 가입자의 호가 해제된 경우(S11), 호 처리부(26)는 세션 종료 통지 메시지를 호 추적부(24)로 송신하고(S12), 호 추적부(24)는 해당 메시지에 포함된 IMSI 또는 IP

주소, TEID를 이용하여 추적 정보 DB(25)에서 관련 데이터를 모두 삭제함으로써 해당 가입자에 대한 추적 기능을 해제하고 이를 운용자에게 보고한다(S13).

<106> 그리고, 호 추적부(24)는 MMI(30)를 통해 운용자로부터 추적 해제 대상 가입자에 대한 정보가 포함된 GTP-U 추적 해제 메시지가 수신되는 경우(S14), 상기 가입자 정보가 포함된 GTP-U 추적 기능 해제 요구 메시지를 호 처리부(26)로 송신한다(S15).

<107> 이에, 호 처리부(26)는 상기 가입자 정보에 포함된 IMSI 또는 IP 주소에 매핑된 TEID를 검색하여 검색된 TEID를 GTP-U 추적 기능 해제 요구 메시지에 저장하여 패킷 처리부(22)로 송신한다(S16).

<108> 그러면, 패킷 처리부(22)는 내부 TEID 테이블에서 해당 TEID에 대한 추적 플래그를 비활성화시켜 GTP-U 추적 기능을 해제하고(S17), GTP-U 추적 기능 해제 응답 메시지를 호 처리부(26)로 송신한다(S18).

<109> 상기 응답 메시지를 수신한 호 처리부(26)는 상기 검색된 TEID가 포함된 GTP-U 추적 기능 해제 응답 메시지를 호 추적부(24)로 송신하고(S19), 호 추적부(24)는 상기 응답 메시지에 포함된 TEID를 이용해 추적 정보 DB(25)에서 관련 데이터를 모두 삭제함으로써 해당 가입자에 대해 GTP-U 추적 기능을 종료한다(S20).

<110> 또한, 본 발명에 따른 실시 예는 상술한 것으로 한정되지 않고, 본 발명과 관련하여 통상의 지식을 가진 자에게 자명한 범위 내에서 여러 가지의 대안, 수정 및 변경하여 실시할 수 있다.

【발명의 효과】

- <111> 이상과 같이, 본 발명은 추적 대상 가입자의 TEID를 이용해 해당 가입자의 GTP-U를 추적함으로써, 실제 가입자 데이터인 GTP-U 메시지에 할당된 GTP 자원을 파악할 수 있는 효과가 있다.
- <112> 나아가, GTP 자원 파악을 통해 SGSN에서 발생하는 패킷 장애에 용이하게 대처할 수 있고, 인터넷 상에서의 GTP-U를 통한 DDOS 등의 공격에 대해서 해당 공격이 발생하는 인터페이스만을 격리시킴으로써 효과적으로 대처할 수 있다.
- <113> 또한, 추적 기능 지속 시간과 추적 임계값을 통해 자동으로 GTP-U 추적을 중지시킴으로써 시스템에 발생할 수 있는 처리 성능 저하를 방지할 수 있다.

【특허청구범위】**【청구항 1】**

추적 대상 가입자의 TEID를 이용하여 상기 가입자 메시지의 점유 자원에 대한 추적 기능을 설정하는 단계; 및

상기 추적 기능이 설정된 가입자 메시지를 검출하여 해당 점유 자원에 대한 정보를 출력하는 단계를 포함하는 것을 특징으로 하는 지티피 자원 추적 방법.

【청구항 2】

제 1항에 있어서,

상기 추적 기능을 설정하는 단계는, 호 추적부에서 운용자로부터 수신되는 상기 가입자에 대한 추적 정보를 호 처리부로 송신하는 단계;

상기 호 처리부에서 상기 추적 정보를 이용해 상기 가입자에게 할당된 TEID를 검색하는 단계;

상기 TEID를 이용해 패킷 처리부에 상기 가입자 메시지 추적 기능을 등록하고 상기 TEID를 호 추적부로 송신하는 단계; 및

상기 호 추적부에서 상기 TEID를 상기 추적 정보와 함께 추적 정보 DB에 저장하는 단계를 포함하는 것을 특징으로 하는 지티피 자원 추적 방법.

【청구항 3】

제 2항에 있어서,

상기 추적 정보는, 상기 가입자의 IMSI, IP 주소, 가입자 메시지 추적을 지시하는 추적 타입 및 추적 대상 메시지의 최대값인 추적 임계값 정보를 포함하는 것을 특징으로 하는 지티피 자원 추적 방법.

【청구항 4】

제 2항에 있어서,

상기 추적 정보 DB에는, 추적 정보, TEID 및 추적된 메시지 개수인 추적 카운트값이 저장되는 것을 특징으로 하는 지티피 자원 추적 방법.

【청구항 5】

제 2항에 있어서,

상기 TEID 등록은, 상기 패킷 처리부에서 상기 TEID와 추적 정보를 수신하는 단계; 및 내부 TEID 테이블에서 해당 TEID 필드의 추적 플래그를 활성화시키고 상기 추적 정보를 저장하는 단계를 포함하는 것을 특징으로 하는 지티피 자원 추적 방법.

【청구항 6】

제 1항에 있어서,

상기 점유 자원 정보를 출력하는 단계는, 패킷 처리부에서 트래픽되는 가입자 메시지의 TEID를 확인하는 단계;

상기 확인된 TEID로 내부 TEID별 테이블을 검색하여 상기 TEID의 추적 플래그 활성 여부를 확인하는 단계;

상기 추적 플래그가 활성 상태인 경우 상기 가입자 메시지의 점유 자원에 대한 정보를 상기 TEID와 함께 호 추적부로 송신하는 단계; 및

상기 호 추적부에서 상기 TEID를 이용해 상기 점유 자원 정보를 운용자에게 출력하는 단계를 포함하는 것을 특징으로 하는 지티피 자원 추적 방법.

【청구항 7】

제 6항에 있어서,

상기 점유 자원 정보는, 상기 가입자 메시지가 트래픽되는 AMA 번호, 인터페이스 번호, VPI/VCI, 링크 대역, 상기 데이터의 스트림 방향성 지시값 및 추적 카운트값을 포함하는 것을 특징으로 하는 지티피 자원 추적 방법.

【청구항 8】

제 6항에 있어서,

상기 점유 자원 정보를 운용자에게 출력하는 단계는, 상기 호 추적부에서 추적 정보 DB를 검색하여 상기 TEID가 저장되어 있는지 여부를 확인하는 단계;

상기 TEID가 저장되어 있는 경우 상기 점유 자원 정보를 상기 TEID에 대응하는 가입자 추적 정보에 매핑시켜 운용자에게 출력하는 단계;

상기 호 추적 정보 DB에서 추적 카운트 값을 증가시키고, 기저장된 추적 임계값과 비교하는 단계; 및

상기 추적 카운트 값이 상기 추적 임계값과 동일한 경우 상기 추적 정보 DB에서 상기 TEID 및 대응하는 추적 정보를 삭제하는 단계를 포함하는 것을 특징으로 하는 지티피 자원 추적 방법.

【청구항 9】

제 2항에 있어서,

상기 추적 정보에 해당 추적 기능을 지속할 시간 정보가 포함되어 있는 경우, 상기 호 추적부에서 상기 TEID 수신시 상기 지속 시간에 대응하는 타이머를 구동시키는 단계를 더 포함하는 것을 특징으로 하는 지티피 자원 추적 방법.

【청구항 10】

제 9항에 있어서,

상기 타이머가 만료하는 경우, 상기 호 추적부에서 상기 추적 정보 DB의 상기 TEID 및 대응하는 추적 정보를 삭제하여 해당 가입자 메시지 추적 기능을 해제하는 것을 특징으로 하는 지티피 자원 추적 방법.

【청구항 11】

제 1항에 있어서,

상기 가입자의 호가 해제되는 경우, 상기 설정된 추적 기능을 해제하는 단계를 더 포함하는 것을 특징으로 하는 지티피 자원 추적 방법.

【청구항 12】

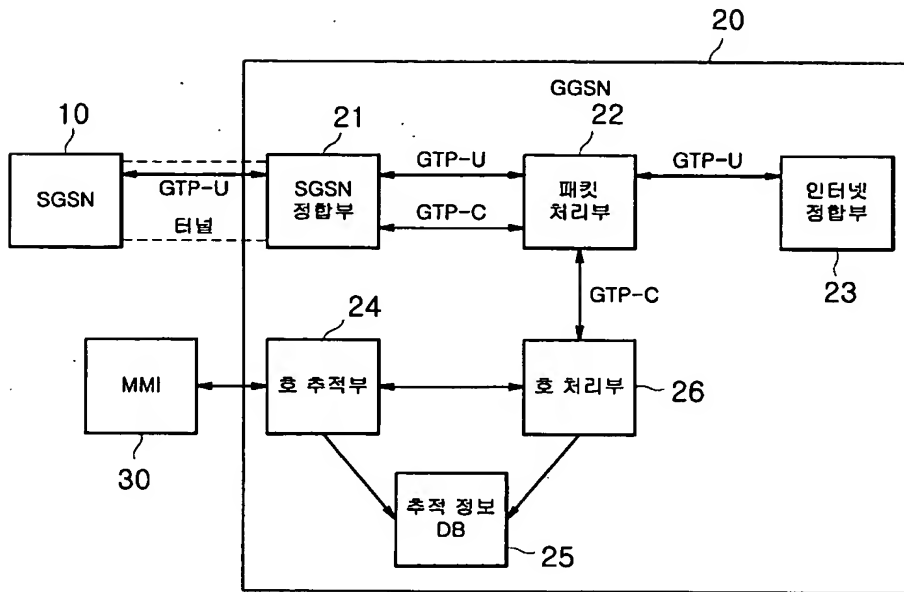
제 11항에 있어서,

상기 추적 기능을 해제하는 단계는, 호 처리부에서 상기 호 해제된 가입자의 식별 정보가 포함된 세션 종료 통지를 호 추적부로 송신하는 단계;

상기 호 추적부에서 상기 식별 정보를 이용해 추적 정보 DB의 해당 TEID 및 추적 정보를 삭제하여 상기 가입자 메시지 추적 기능을 해제하는 단계를 포함하는 것을 특징으로 하는 지티피 자원 추적 방법.

【도면】

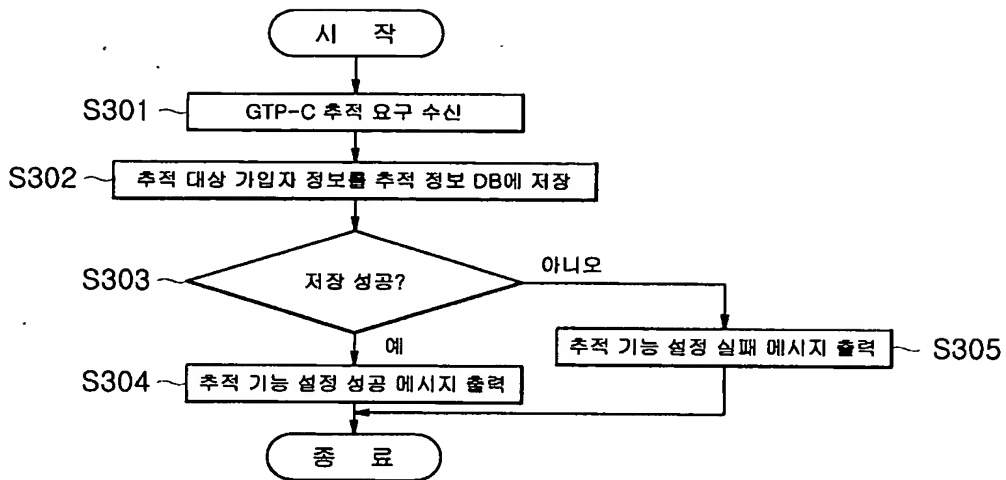
【도 1】



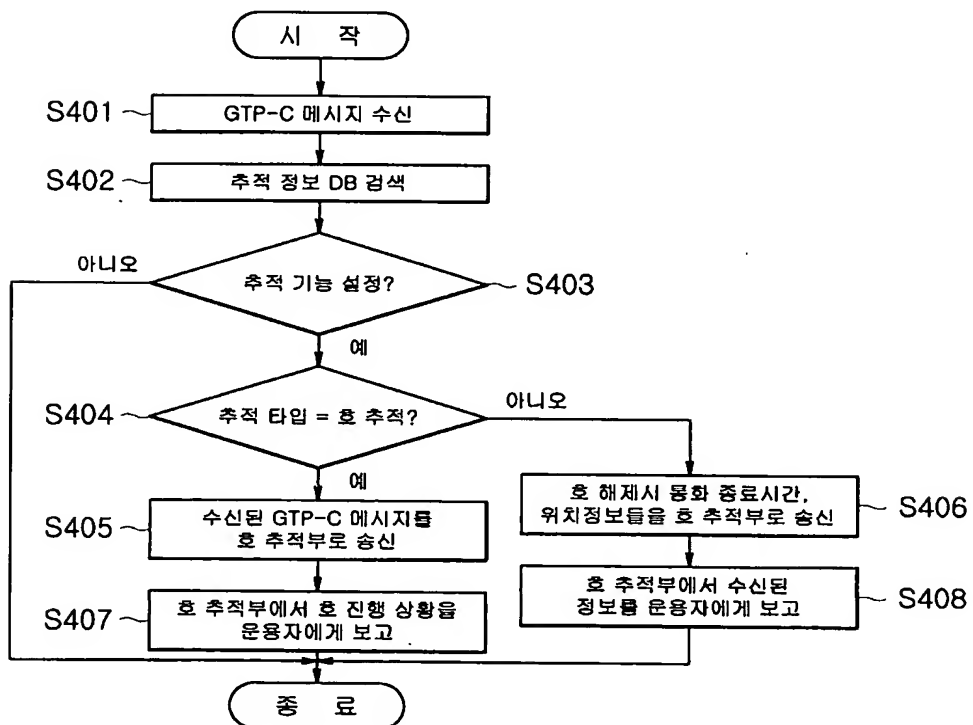
【도 2】

Attribute	자료형
INDEX	추적 정보 Index
IMSI	추적 대상 가입자의 번호
IMSI_CNT	가입자 번호 자리수
IP_ADDR	추적 대상 가입자의 IP 주소
TRC_TYPE	현재 설정된 추적 타입

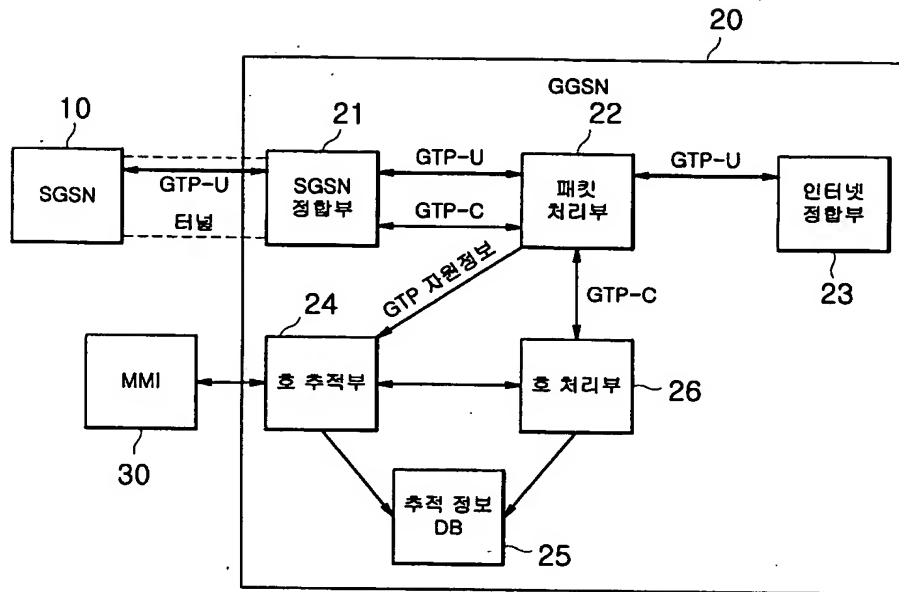
【도 3】



【도 4】



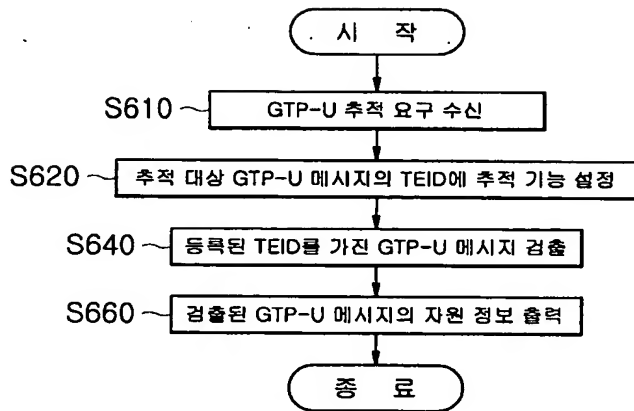
【도 5】



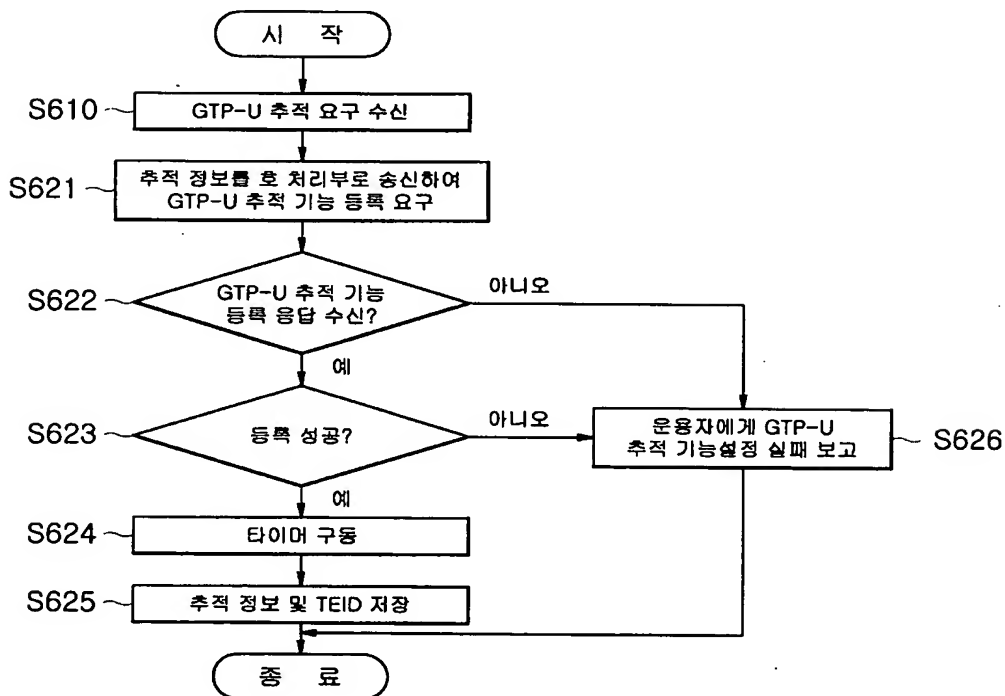
【도 6】

Attribute	자료형
INDEX	추적 정보 인덱스
IMSI	추적 대상 가입자 번호
IMSLCNT	가입자 번호 자리수
IP_ADDR	가입자 IP 주소
TRC_TYPE	현재 설정된 추적 타입
TEID	터널 식별자
DURATION	추적 기능 지속 시간
Up/Down stream LMT	추적 임계값
Up/Down stream CNT	추적 카운트 값
TIMER_ID	타이머 식별자

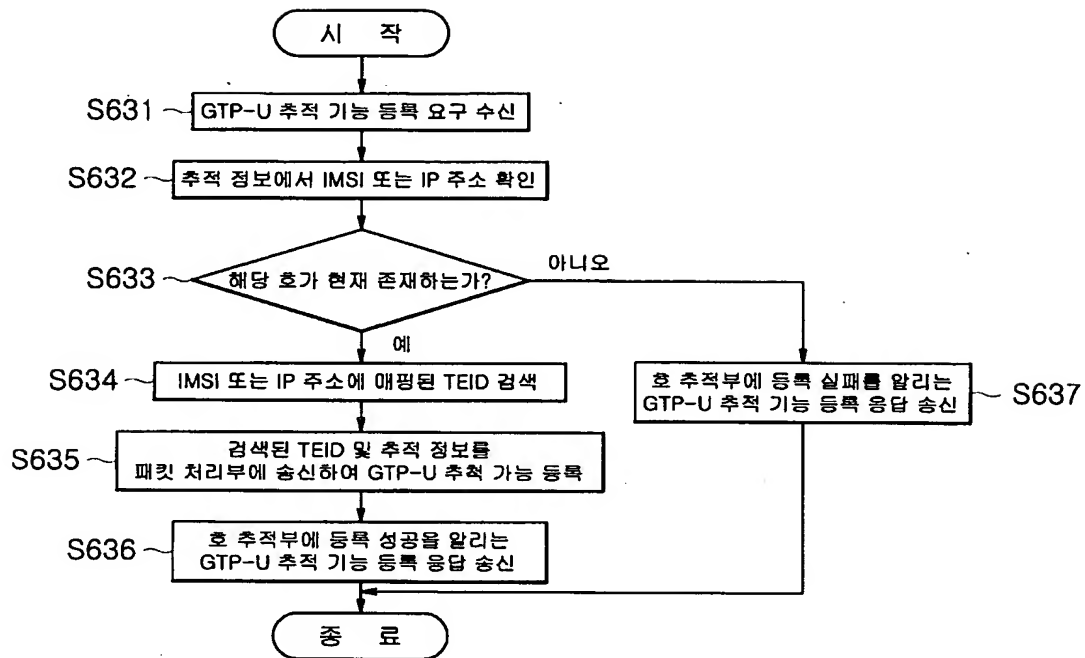
【도 7】



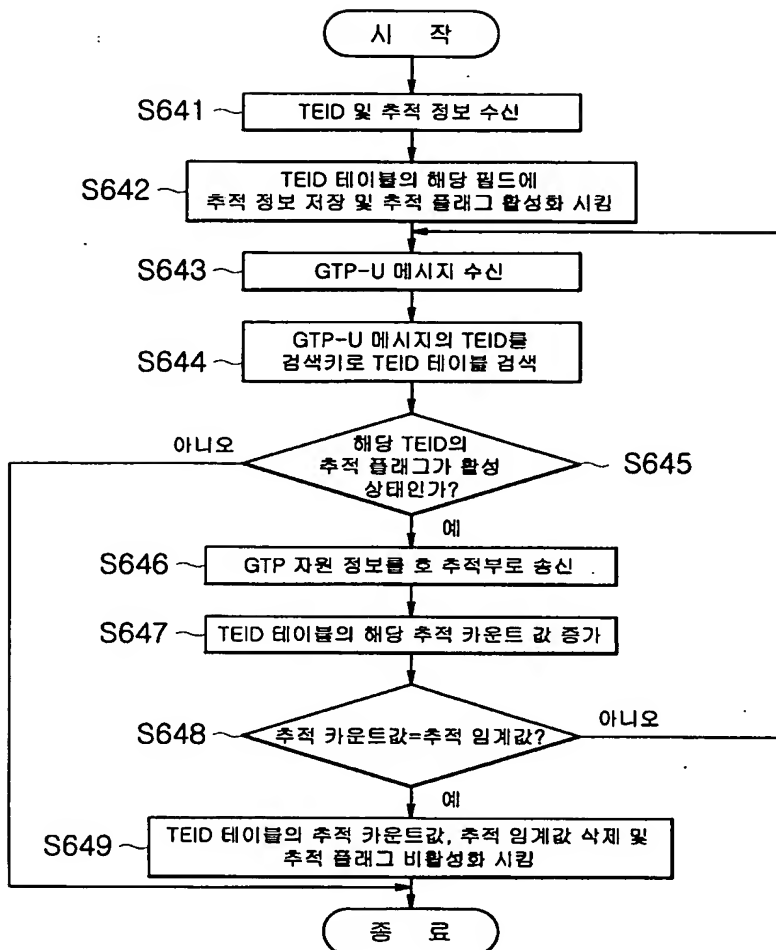
【도 8】



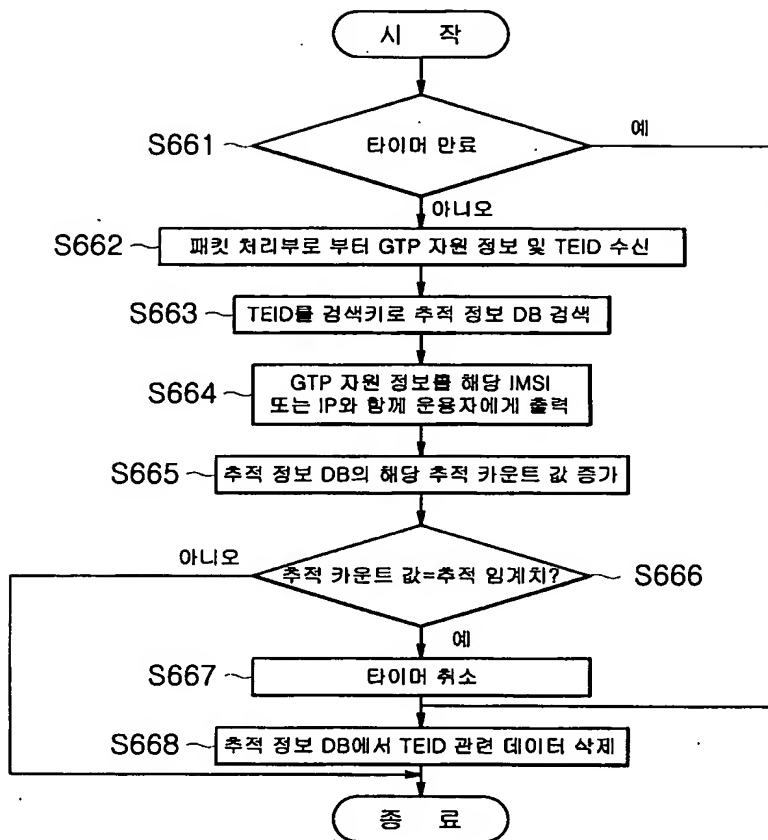
【도 9】



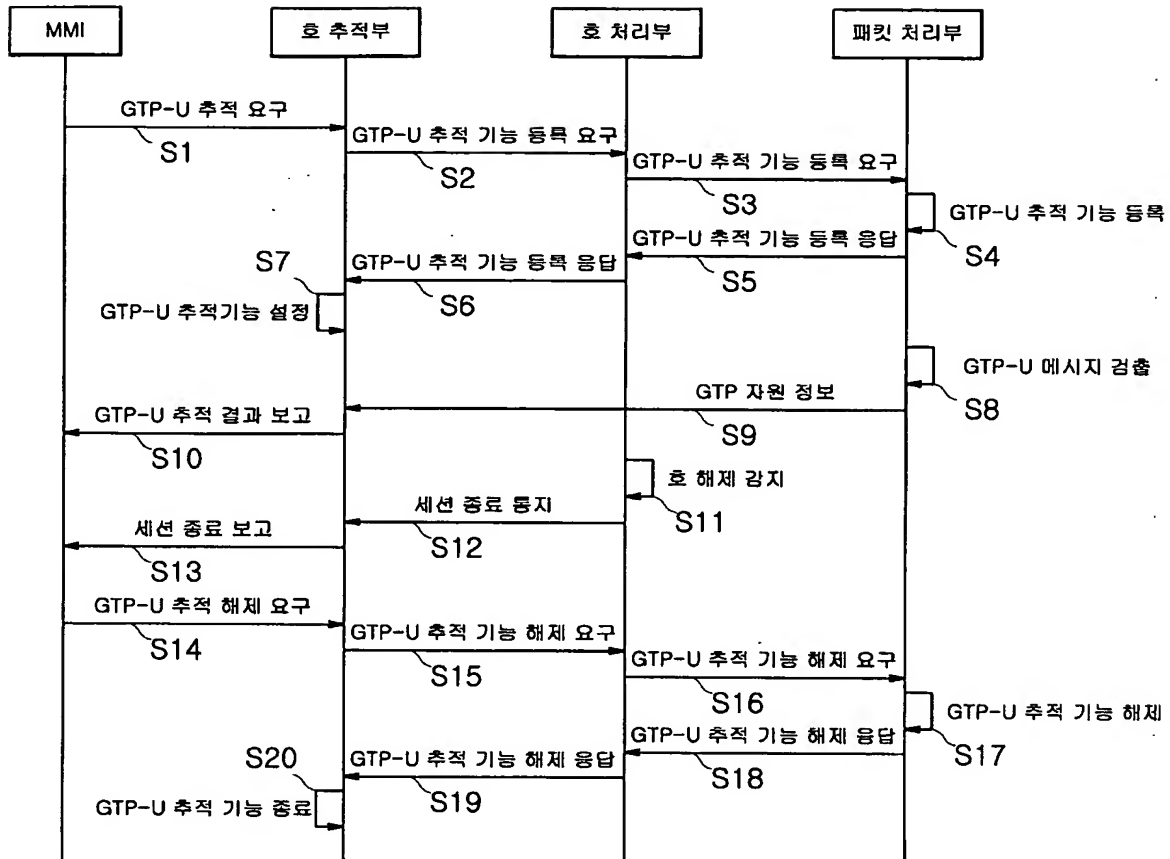
【도 10】



【도 11】



【도 12】



THE ESCHER & KIM
100 BOY
100 BOY